Efficient Secured Two Party Computing with Encrypted Data for Public Cloud

L.Kalaivani, Dr.R.Kalpana

Abstract— In this project we intervened certificateless encryption plan without matching operations for safely imparting public cloud. Intervened certificateless open key encryption (mCL-PKE –Mediated certificateless public key encryption) takes care of the key escrow issue in identity based encryption and testament repudiation issue in public cloud key cryptography. In existing mCL-PKE plans are wasteful in utilization of costly blending operations or helpless against incomplete unscrambling assaults. With a specific end goal to address the execution and security issues, in this project, we first propose a mCL-PKE plan without utilizing matching operations. We apply our mCL-PKE plan to develop a down to earth answer for the issue of offering touchy data out in the open mists. The cloud is utilized as a protected stockpiling and a key era focus. In our framework, the information manager scrambles the delicate information utilizing the cloud produced clients' open keys focused around its get to control arrangements and transfers the scrambled information to the cloud. Upon effective approval, the cloud incompletely unscrambles the encoded information for the clients. The clients in this manner completely unscramble the halfway decoded information utilizing their private keys. The secrecy of the substance and the keys is safeguarded as for the cloud, in light of the fact that the cloud can't completely unscramble the data. We additionally propose an augmentation to the above methodology to enhance the effectiveness of encryption at the information manager. Finally we execute our mCL-PKE plan and the general cloud based framework with the help of proxy, in order to access data if users lost their certificate or key.

***Index Terms*— Cloud Computing, Proxy Re- encryption, Attribute based Encryption,Cloud Security**

I. INTRODUCTION

Cloud computing is a term for any thing that involves delivering services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a- Service(IaaS), Platform-as-a-Service (PaaS) and Software-as- a-Service(SaaS).The name cloud computing was stimulated by the cloud symbol that's used to represent the Internet in network diagrams.Cloud as awhole is not a new technology that has emerged ,but it has used all other boomed technologies in recent years to provide the best of all services.

Cloud came into reality using a method called Virtualization.Virtualization is nothing but an abstract of the resources that are available. The Infrastructure-as-a-Service(IaaS) provider likeAmazon Web Services provides virtual server instances with unique IPaddresses and provides blocks of storage on demand. Customer susethe provider's Application Program Interface(API) to start,stop,access and configure their virtual servers and storage.

Currently the secured data storage mechanism in cloudisstill in surfacing stage and it is not very popular across organization and individual users. Primary reasons of low usage are data security and Internet availability. The computational cost for pairing is high compared to other standard operations. Mediated certificate less pulic key encryption (mCL-PKE) scheme avoids the pairing operations. The certificate management is very expensive and complex. It reduces the certificate management complexity. It is secured against partial decryption attacks. The data canbe encrypted once for several users and avoids the overhead of the data owner. It guarantees the validity of user's public key without the certificate. The sharing of secure data is achieved by this scheme.

II.RELATEDWORKS

"Attribute Based Encryption (ABE) RSA algorithm" [1]in this access control system, each cipher text is lRSAled by encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of cipher texts the key can decrypt. It only permits an authority to issue private keys that express threshold access policies, in which a certain number of specified attributes need to be present in the cipher text in order for a user to decrypt.

Access tree structure is used to construct the key. In the tree construction, each non leaf node represents a threshold gate and leaf node of the tree is described by an attribute and threshold valueas1.The cipher texts are provided with a set of descriptive attributes. Private keys re identified by a tree- access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. A user will be able to decrypta ciphertext with a given key if and only if there is an assignment of attributes from the cipher texts to nodes of the tree such that the tree is satisfied. Once the key is obtained, re-randomization is applies over the key using random polynomial.

Manuscript received March 19, 2015

L.Kalaivani, Department of Computer Science & Engineering, IFET College of Engineering.

Dr.R.Kalpana, Professor, Department of Computer Science & Engineering, IFET College of Engineering.

"KeyPolicy-Attribute based encryption (KP-RSA)"[3].This technique was introduced byGoyalet.al.to provide access control in the cloud environment.For the purpose of helping the data owner to enjoy fine-grained access control of data stored on untrusted cloud servers, a feasible solution is provided by encrypting data through certain cryptographic primitives, and is closing decryption keys only to authorized users. Unauthorized users, including cloud servers, are not able to decrypts ince they do not have the data decryption keys. It uses Decision albi linear Diffie-Hellman assumption long with the linear secret sharing scheme. It considers the non-monotone attributes forassigningpolicies.Onecriticalissueinthis approachishowtoachievethedesiredsecurity goalswithout introducingahighcomplexity onkeymanagementanddata encryption. Toresolvethisissue,perfileAccessControlList (ACL)forfine-grainedaccesscontrolisintroduced.Several filegroupsforefficiency.Asthesystemscales,however, the complexityoftheACL-basedscheme would beproportionalto the number of users in the system. The file group-based scheme,onthe otherhand,is just able to providecoarse-graineddataaccesscontrol.Itactuallystillremainsopen tosimultaneously achievethegoalsoffine-grainedness, scalability,anddataconfidentiality fordataaccesscontrolin cloudcomputing.

"CiphertextPolicy-Attributebased encryption (CP-RSA)"[4].Thistechniqueisproposed by"JohnBethencourt et.al".Inthiseachuserisassociated withasetofattributes. Usersecretkeyisassociated withanaccessstructure. Dataare encryptedoverasetofattributes.Decryption ofdatarequires thedataattributestosatisfytheuseraccess structure.To detect illegal user, their identities IDs should be included in the privatekeyofattributelistL.ThereisnouserIDinformation intheciphertext.Thisschememakesuseofbilinear map assumptionswheretheattributeisattachedtotheprivatekeyof thedifferentusers.Ittakestheadvantage ofownerhavingthe controlofdistribution ofdata.Itisresistanttomultiple collusionattack.

"Hierarchical AttributeSetBasedEncryption"[10] ThisRSAisproposedbyZhiguoWanet.al forprovidingaccesscontrol. TheRSAmodelconsistsofa rootmaster(RM)thatcorresponds tothethirdtrustedparty (TTP),multipledomainmasters(DMs)inwhomthetop-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. The RM, whose role closely follows the root Private key Generator (PKG) RSA system is responsible for the generation and distribution of system parameters and domain keys.

The DM, whose role integrates both the properties of the domain PKG in a HIBE system and in a CP-RSA system, is responsible for delegating keys to DMs at the next level and distributing keys to users. The leftmost DM enable the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. The other DMs administer an arbitrary number of disjoint attributes, and have full control over the structure and semantics of their attributes. In the RSA model, each DM and attribute is assigned a unique identifier (ID), but marks each user with both an ID and a set of descriptive attributes. Then an entity's secret key is extracted from the DM administering itself, and an entity's public key, which denotes its position in the RSA model, to be an ID tuple consisting of the public key of the DM administering itself and its ID, e.g., the public key of DMi with IDiis in the form of (PKi−1; IDi), the public key of user U with IDu is in the form of (PKu-1; IDu), where PKi−1, PKu-1are assumed to be the public keys of the DMs that administer DMi, U respectively.This scheme uses ciphertext policy based encryption along with the hierarchical identity based encryption. It provides unique identifier to each user along with their descriptive attribute structure.

III. System Structure

A system structure of privacy preserving cloud storage using mCL-PKE scheme is

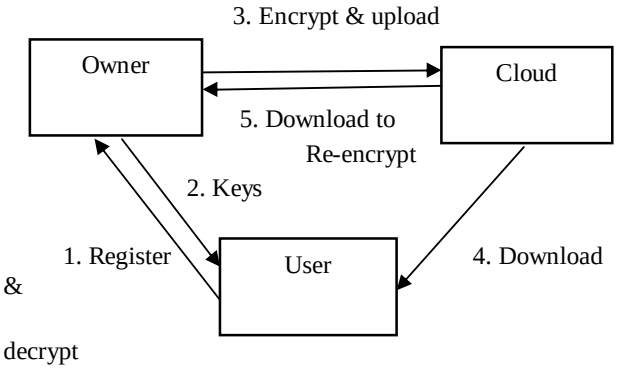

Fig1:SystemArchitecture

As shown in figure 1 the scheme consists of three major entities: owner, cloud, user. Data owner will receive the registration request from the user. Then the request is forwarded to the cloud. After registration key is generated and stored in public cloud. Data owner can encrypt the data and stores the encrypted data. In our scheme RSA algorithm is used for encryption. User can login into the account and runs the algorithm using his private key. Then the user can decrypt the data. Proxy is supported in order to access data if user lost his key or certificate. The login details can be regenerated through the proxy.

In dynamic scenario users may join or leave and group structure will be changing often. The key that has todevised for specific user should have validity only till the member remains in the group,otherwise key should get expired. Moreover attributes cannot be defined unique for each user and one-to-one mapping between user and attributes cannot be done.

IV.SecurityOutline

In this proposed system, it allows any user to have their data secured through encryption amongs teach data is shared between different sharers according to the control what they have on data.It uses proxyre-encryption scheme that emphasis security to be given by cloud leveraging the work done by the user.To achieve this,hierarchical identity role based proxyre-

encryptionschemeisproposed.Itallowsausertoencrypt his dataunderhisidentity toprotecthisdatafromleakingand,at thesametime,todelegatehisdatamanagementcapabilityto thecloud.Furthermore theusercoulddelegate hisaccess controlcapabilitytothecloud,whichcouldgranttheaccess of anauthorizeduserundertheroleheplays,consideringhis placeinhishierarchy,andbytransforming theciphertext encryptedwiththedataowner'sidentity totheonewiththe sharer'sidentity.

Thedatasharer,whohadalready registeredwithdata owner,isprovidedwiththesecretkey.Thatsecretkey isused for proxy re-encryption scheme by the cloud. So that the sharers inthefutureusingtheirsecretkey generated could decryptdatabasedon their identity.The differentsharer's identitycorresponding todifferentproxyre-encryptionkeyis generatedatthetimeoftheirregistration.Whenthe dataowner providestheproxyre-encryptionkeytothecloud,thecloud canconvertthciphertext outsourced bythedataownertothe ciphertextthatcanbedecryptedbythe sharers.

Theillustration isgiven inTable1.Inthisthedata owner uploads the encrypted file to the cloud. Then the cloud performstheProxy-Re-encryption usingthesharer'sidentity andstoresitinthedatabase.Whenevertheuserwantstoaccess thefileheretrievesitbydecrypting thefileusinghissecret identity.

Table1:TaskSchedule

DataOwner	Cloud	DataSharer
Encryptsdata	Stores Data givenbydata owner	Registers itself for Authorization with Data Owner
Authorizes datasharer	Applies Proxy Re-encryption	Requestsdata fromcloud
Provides secretkey	Sendsdatato theSharer	Decrypts the datausingits secretkey

A.SystemSetup:

Inthisphase,importanttasksaredone.Initially security parameter istakenasinput.Ithelpstodesigntheaccesstree under which the message is encrypted. It outputs the parameterspublicandprivatekey(PUa,PRa).Each userinthe system isassociatedwithaccessstructurewhichspecifiesthe attributesassociatedwiththeusersdecryptionkey.

B.KeyGeneration.

Therandomalgorithmwhichtakesthesetofattributes Attiand PrivateKey PRaasinput andoutputs thekey DKbfor decryptionbasedon setofattributesinthelist.

C.DataEncryption:

TherandomalgorithmwhichtakesPublickey,MessageM andaccessTreeasinputoverthesetofattributes. The CiphertextCiisproduced. Theciphertextindeedwillcontain theaccessstructurewithinitfor decryption.

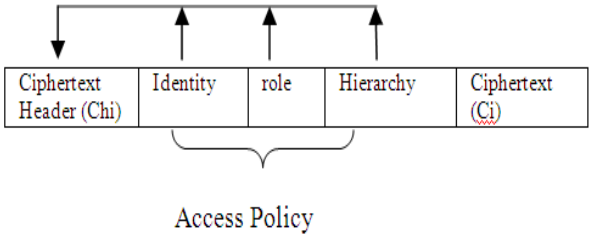

Fig2:FileStructure

$$Ci=(PUa;E(PRa,M))(1)$$
$$Ci=(PUa,AS:(ID,R,H)) \quad (2)$$

Thekeysforencryptionaregeneratedwheneverthedataowner choosesafileforuploading.Thedataownerencryptsthedatabasedonpublickeyparameters andaccessstructureisdefined overtheciphertext usingtheciphertext header.Afterthedata beingplacedinthecloud,thecloudservice providerwill performtheproxyre-encryptionovertheencrypteddata.

D.Datasharing:

Inthisphasetheproxyre-encryption schemeallowsthegiven proxyre-encryption keytotranslatetheciphertextwhichis encryptedunderPUaintociphertextofthedatasharerunder thetheir publickey.Eachsharerhasto registerwiththesystem andobtaina secretkeycorrespondingto hisidentityandrolein the hierarchy,

$$sk=Hash(ID+role)=HIRBE(IDRu) \quad (3)$$

The secretkeyisgeneratedastheHash functionofthesharer's identity.There-encryptionkeyskwillbeusedbythecloudto transform theciphertextCitotheciphertextundersharer's secretkey.

Thedataownerneednotbeonline alwayssothedataowner forwards sktothecloudwhichmeansthatthecloudis delegatedto managethedataonbehalfoftheowner.Thecloud candeploy there-encryptkeysktopermittheauthorizeduser togetthciphertextdecryptedwithhisownsecretkey.

E.Dataaccess:

Thedatasharerinitially generatesthedatafilerequesttothe cloudserver.Thecloudserverwhichmaintains thesecretkey on behalf of the data owner will sendtherequested datatothe

data sharer. The data sharer will decrypt the file using the secre tkey.

Ci=(E(IRBE(IDs),(c(f))))=(E(sk,(F.e(PRa))))(4)

Then the sharer fetches there-encrypted data from the cloud servers, and runs the Decrypt algorithm on Mi with his secret key to obtain the

D(F)=C(F)=Dec(sk,C) (5)

Then for obtaining the original file uploaded by the owner, the user have to perform another decryption using the owner's publickey(PUa). The original file is generate das

F=Dec(PUa,D(F)) (6)

Any sharer can obtain the required file with the permission of the data owner.

V.RESULTANALYSIS

The implementation uses the cpRSA toolkit that use spairing– Based Cryptography library.The data owner encrypts a file to create a new encrypted file. The time required for the operation depends on the access tree and key structure. The number of attributes is assumed to be 30 and the relation between number of attributes and key generation time is compared. Also number of attributes and the decryptiontime is compared.

Table 2 : No. of Grant

Number of Attributes	Key Generation Time (s)	Authority Grant
10	0.2	2
20	0.4	5
30	0.6	6
40	0.8	9
50	1.0	11

The table2 shows the number of authorization grant given by the higher authority considering different number of attributes for various key generation time.

Figure 3 shows the encrypted file storage in the cloud.

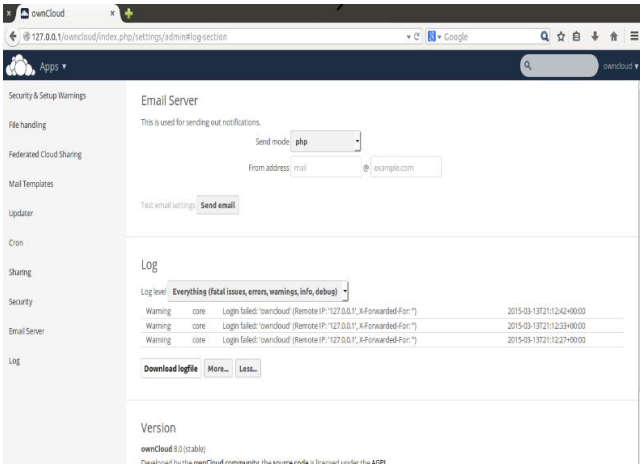

Fig3: OUTPUT SCREEN

VI.CONCLUSION&FUTURE SCOPE

In this paper, Hierarchical, identity and role attribute based encryption scheme is explored. It offers fine-grained access control of data and also guarantees the data privacy in the cloud. The communication and computation cost of the user is highly reduced since the proxy encryption and secret key allocation is pushed to cloud service provider side. The scheme also lets the data owner not to be online always. At the same time, the cost of updating of access policy and communication is also reduced in this mechanism. Each user has an identical key based on their identity there will be no duplicates. Each user is registered with the administrator and the user only knows the secret key and owner there will be no unauthorized access. As the data is forwarded to the cloud in encrypted format, it does not have any knowledge about the data. Though the intruders get the data from the cloud they cannot decrypt the data. As the encrypted data as the double wrapping is done over the data and keys are only transferred once that lets the computation cost to be comparatively low. There is no limitation imposed on the number of the data sharer.

VII. REFERNCES

[1] V.Goyal,O. Pandey,A.Sahai,andB. Waters, "Attribute- based encryptionforfine-grainedaccesscontrol of encrypted data," in CCS,ACM, 2006,pp.89–98.

[2] S.Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,andfine-graineddata access controlincloud computing," inINFOCOM, 2010,pp.534–5.

[3]R. Ostrovsky,A. Sahai, and B. Waters, "Attribute-based encryptionwithnon-monotonic accessstructures,"inACM Conference onComputer andCommunications Security, 2007, pp.195–203.

[4] BethencourtJ, SahaiA,WatersB."Ciphertext-policyattribute basedencryption".In:Proceedings ofISSP;2007,pp. 321-34.

[5] BonehD,FranklinM.,"Identity-basedencryptionfrom theWeil pairing". In: Proceedings of CRYPTO. LNCS, vol. 2139; 2001,pp.213-29.

[6]Y.Zhu, H.Hu, G.-J.Ahn, D.Huang, and S.Wang, "Towards Temporal Access control inclouds," in Proc.IEEE INFOCOM, 2012,pp.2576-2580.

[7] Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM,IEEE, 2010, pp. 534–542.

[8] Y. Zhu, H. Hu, G.-J. Ahn, M. Yu, and H. Zhao, "Comparison-based encryption for fine-grained access control in clouds," in CODASPY, ACM, 2012, pp. 23-55.

[9] A.Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT, Springer, 2005, pp. 457–473.

[10] Zhiguo Wan, Jun'e Liu, Robert H. Deng,"HASBE: A Hierarchical Attribute - Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensincs and Security, Vol. 7, NO. 2, April 2012, pp. 67-90.

[11] Tim Mather, Subra Kumaraswamy, shahed Latif, "Cloud Security and privacy: An Enterprise respective of risk and compliance Theory in practice" , 2012, pp. 98- 105.